REMARKS

Claims 1-6, 8-12, and 14-23 are pending. No claim amendments are made with this response. Reconsideration of the application is respectfully requested based on the following remarks.

I. REJECTION OF CLAIMS 1-6, 8-12, and 14-23 UNDER 35 U.S.C. § 103(a)

Claims 1-6, 8-12, and 14-23 were rejected under 35 U.S.C. § 103(a), as being unpatentable over U.S. Patent No. US 6,963,946 B1 Dwork et al. (Dwork) in view of U.S. Patent No. US 7,274,792 B2 Chin et al. (Chin). Withdrawal of the rejection is respectfully requested for at least the following reasons.

i. Neither Dwork nor Chin teach a security system that is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system, as recited in independent claims 1 and 15.

Independent claim 1 recites a network interface system that is adapted to obtain initialization vector information from the host system and provide the initialization vector information to the security system, ***wherein the security system is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system.***

The Office Action dated 9/30/2008 (see page 4, paragraph 3) admits that Dwork does not teach *"wherein the security system is adapted to employ an initial random data string from the outgoing data to begin encryption before security association information has been retrieved by the security system."* Accordingly, the Office Action further cites the Cryptography Accelerator 201 of Fig. 2 of Chin and a related description of Fig. 2 from Column 4, lines 10-14 of Chin, which states: *"The controller derives information from data received from the host and provides the information along with context such*

as algorithm information, initialization values, and keys to the various encryption and authentication engines." (O.A., 9/30/08, p. 4, paragraph 3).

However, this description of Fig. 2 of Chin further states (Column 4, lines 21-29) that: *"In typical implementations, a secured connection typically includes* ***a handshake phase and a data transfer phase****. Any connection between two entities exchanging encrypted data using the same key or a set of keys is referred to herein as a secure connection or a secured connection. ...* ***Data transfer*** *typically occurs* ***after the handshake phase is completed*** *and command information is established for the secure connection."* And (Column 4, lines 36-39) states: *"****After*** ***a secure connection is established, a first entity can transmit packets*** *to a second entity using the* ***secure connection and the security association****."*

Clearly, therefore, the completion of the secured connection **handshake phase** of Chin is marked by the transmitting of data packets in the **data transfer phase** which uses the **secure connection and the security association**, and after which encryption may begin. By contrast, the security system of the present invention employs the **initial random data string** to begin encryption **before the security association information has been retrieved**. The present invention employs the **initial random data string** during a time which appears to be more comparable to the **handshake phase** of Chin and **before the data transfer phase**. Thus, Chin does not teach the retrieval or use of the **security association** information or the initialization vector information from the host system until later during or after the **data transfer phase**.

Thus, neither Dwork nor Chin disclose the features recited in claims 1 and 15. Therefore, Applicant respectfully submits that independent claims 1 and 15, and the claims which depend therefrom, respectively, are non-obvious, and therefore patentable over Dwork in view of Chin. Withdrawal of this rejection is therefore respectfully requested.

In addition, Claims 10 and 11, for example, further recite that the security system selectively employs an initialization vector (IV) (*e.g.*, 226 of Fig. 1F) comprising the initial random data string from the outgoing data to perform CBC encryption according

to the initialization vector information, wherein the security system is adapted to use the initial random data string as **a seed value for encrypting the first block of cyphertext before the security association information has been retrieved by the security system.** (See, *e.g.*, Applicants' specification page 16, lines 12-13, 24-28).

Further, although the descriptor management system 130 of Dwork also comprises initialization vector length bits IVLEN0 and IVLEN1 in the TFLAGS1 byte 193 of transmit descriptor 192a (*e.g.*, col. 24, ll. 54-59, and Figs. 5E and 5F), such length bits of Dwork are not "inherently" initialization vectors (*e.g.*, IV 226) comprising a random data string that can be used by the security system to facilitate high-speed data encryption **before security association information has been retrieved by the security system.**

In one non-limiting example, the inventors have appreciated that in network interface systems, such as the systems 2 and 102 described in the present invention, in which security processing is performed outside the host system 6, that the security processing system 124 must be able to differentiate between outgoing data frames 200 that include an IV 226 (*e.g.*, as illustrated in Fig. 1F) and those that do not (Fig. 1E). In the example systems of the present invention, initialization vector information 191 is provided to the security processing system 124 by the descriptor management system 130, to indicate whether an IV 226 is present in the frame 200, and if so, the length of the IV 226. Although such information may be derived from the security association (SA) associated with a particular data frame 200, the provision of the information 191 by the descriptor system 130 advantageously allows the encryption to begin before the SA information has been retrieved by the security processor 174, thus facilitating high-speed data encryption to meet gigabit wire speeds.

Therefore, Applicant respectfully submits that independent claims 1 and 15, and the claims which depend therefrom, respectively, are patentable and not anticipated by Dwork in view of Chin. Withdrawal of this rejection is therefore respectfully requested.

II. CONCLUSION

For at least the above reasons, the claims currently under consideration are believed to be in condition for allowance.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Should any fees be due as a result of the filing of this response, the Commissioner is hereby authorized to charge the Deposit Account Number 50-1733, AMDP763US.

Respectfully submitted,
ESCHWEILER & ASSOCIATES, LLC

By /Thomas G. Eschweiler/
Thomas G. Eschweiler
Reg. No. 36,981

National City Bank Building
629 Euclid Avenue, Suite 1000
Cleveland, Ohio 44114
(216) 502-0600